

(1) Bezout theorem proof and Example (inverse of 101 mod 4620)

Bezout Theorem : if a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. Where s and t are called Bezout co-efficient of a and b .

Finding the inverse of 101 mod 4620

$$\therefore 101x \equiv 1 \pmod{4620}$$

$$\therefore 101x + 4620 = 1$$

Apply Euclidian Algorithm,

$$4620 = 45 \times 101 + 75$$

$$101 = 75 \times 1 + 26$$

$$75 = 2 \times 26 + 23$$

$$26 = 23 \times 1 + 3$$

$$23 = 3 \times 7 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

$$\therefore \gcd(101, 4620) = 1$$

(11) Fermat Little Theorem:

If p is prime and a is an integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore,

for every integer a we have

$$a^p \equiv a \pmod{p}$$

Finding $7^{222} \pmod{11}$

By Fermat's Little Theorem we know that,

$$7^{10} \equiv 1 \pmod{11}$$

$$(7^{10})^k \equiv 1 \pmod{11}$$

$$\text{thus } 7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2$$

$$= (7^{10})^{22} \cdot 49$$

$$= (1)^{22} \cdot 49$$

$$= 5 \pmod{11}$$

$$\text{That means } 7^{222} \pmod{11} = 5$$

By working Backward,

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1(23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$

$$1 = -1 \cdot 23 + 8(26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$

$$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$$

$$1 = -9 \cdot 75 + 26(101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$$

$$1 = 26 \cdot 101 - 35(4620 - 45 \cdot 101)$$

$$1 = -35 \cdot 4620 + 1601 \cdot 101$$

\therefore The Inverse of $101 \pmod{4620}$ is 1601

(11) Chinese Remainder Theorem:

Let n_1, n_2, \dots, n_k be pairwise co-prime integers ($\gcd(n_i, n_j) = 1$ for all $i \neq j$) and

let a_1, a_2, \dots, a_k be any integers.

Then, the system of simultaneous

Congruences:

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$\vdots$$

$$x \equiv a_k \pmod{n_k}$$